

CLAIMS

What is claimed is:

- 156  
31  
C1
- 00306989 003159
- Sub  
C1
- Sub  
C3
- 1 ~~1.~~ A method for maintaining a security profile throughout nested service  
2 invocations on distributed components, comprising the steps of:  
3 (a) providing interconnections between distributed components each having  
4 nested service invocations;  
5 (b) identifying a user;  
6 (c) associating the user with roles;  
7 (d) creating a user context instance upon successful identification of the user,  
8 wherein the user context instance includes information about the user  
9 including the roles;  
10 (e) receiving a request from the user to invoke a service on a component,  
11 wherein the component invokes an additional service of another component;  
12 (f) querying the user context for the information about the user;  
13 (g) comparing the user information with an access control list for verifying that  
14 the user has access to the component; and  
15 (h) comparing the user information with an access control list for verifying that  
16 the user has access to the additional service of the other component.
  - 1 2. A method as recited in claim 1, further comprising the step of logging all  
2 user interactions.
  - 1 3. A method as recited in claim 1, further comprising the step of modifying a  
2 user interface to provide access to actions that can be performed by the user  
3 based on an identity of the user and the roles associated with the user.
  - 1 4. A method as recited in claim 1, further comprising the step of passing the  
2 user context instance along as a parameter of service invocations.
- 96

Sub  
C<sub>2</sub>

- 1 5. A method as recited in claim 4, wherein the service invoked associates any  
2 objects created, updated, or deleted with the user context instance.
- 1 6. A method as recited in claim 1, wherein the user context instance  
2 encapsulates security certificates of the user.
- 1 7. A computer program embodied on a computer readable medium for  
2 maintaining a security profile throughout nested service invocations on  
3 distributed components, comprising:  
4 (a) a code segment that provides interconnections between distributed  
5 components each having nested service invocations;  
6 (b) a code segment that identifies a user;  
7 (c) a code segment that associates the user with roles;  
8 (d) a code segment that creates a user context instance upon successful  
9 identification of the user, wherein the user context instance includes  
10 information about the user including the roles;  
11 (e) a code segment that receives a request from the user to invoke a service on a  
12 component, wherein the component invokes an additional service of another  
13 component;  
14 (f) a code segment that queries the user context for the information about the  
15 user;  
16 (g) a code segment that compares the user information with an access control list  
17 for verifying that the user has access to the component; and  
18 (h) a code segment that compares the user information with an access control list  
19 for verifying that the user has access to the additional service of the other  
20 component.
- 1 8. A computer program as recited in claim 7, further comprising a code  
2 segment that logs all user interactions.

Sub B<sup>40</sup>

1 9. A computer program as recited in claim 7, further comprising a code  
2 segment that modifies a user interface to provide access to actions that can be  
3 performed by the user based on an identity of the user and the roles  
4 associated with the user.

1 10. A computer program as recited in claim 7, further comprising a code  
2 segment that passes the user context instance along as a parameter of service  
3 invocations.

Sub A<sup>8</sup>

1 11. A computer program as recited in claim 10, wherein the service invoked  
2 associates any objects created, updated, or deleted with the user context  
3 instance.

Sub C<sup>40</sup>

1 12. A computer program as recited in claim 7, wherein the user context instance  
2 encapsulates security certificates of the user.

Sub A<sup>8</sup>  
Sub B<sup>23</sup>

1 13. A system for maintaining a security profile throughout nested service  
2 invocations on distributed components, comprising:  
3 (a) logic that provides interconnections between distributed components each  
4 having nested service invocations;  
5 (b) logic that identifies a user;  
6 (c) logic that associates the user with roles;  
7 (d) logic that creates a user context instance upon successful identification of the  
8 user, wherein the user context instance includes information about the user  
9 including the roles;  
10 (e) logic that receives a request from the user to invoke a service on a  
11 component, wherein the component invokes an additional service of another  
12 component;  
13 (f) logic that queries the user context for the information about the user;  
14 (g) logic that compares the user information with an access control list for  
15 verifying that the user has access to the component; and

~~Logic that confirms that component.~~

Sub

Sub C  
B<sup>6</sup>

long as

Sub A10

Sub C 1500

[illegible]